Amendments to the Claims

Please amend the claims as indicated in the following listing of claims. This listing replaces all prior listings of the claims.

1. (Currently Amended) A method in a data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

receiving, at a registration manager, a request from a user for a digital certificate, the request including an encryption key associated with the user;

encrypting the user's encryption key with a first archival key;

providing, by the registration manager, the user's encryption key that is encrypted with the first archival key;

storing, by a recovery manager, the encrypted user's encryption key in a database ~~under the control of a first entity separate from the certificate authority~~;

providing, by the recovery manager to the registration manager, an indication of proof of storing the encrypted user's encryption key, wherein the indication of proof is signed with a second archival key;

verifying, by the registration manager, the signed indication of proof based on the first archival key; and

providing, by the registration manager, the request to the certificate authority based on the verification of the signed indication of proof.

2. (Currently Amended) The method of claim 1, further comprising the step of sending a digital certificate from the certificate authority to the user in response to the certificate authority receiving a second request from the registration manager.

3. (Canceled).

4. (Currently Amended) The method of claim 1, further comprising:

encrypting, by a client associated with the user, the request with a transport key; and

sending the transport encrypted request to the registration manager ~~first entity~~.

5. (Currently Amended) The method of claim 4, further comprising:

decrypting, by the recovery manager ~~first entity~~, the transport encrypted request.

6. (Canceled)

7. (Currently Amended) The method of claim ~~6~~1, wherein the second archival key is a data recovery manager private key.

8. (Canceled)

9. (Original) The method of claim 1, wherein the user's encryption key is archived under control of the user.

10. (Currently Amended) A method in a data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

digitally signing, at a recovery manager, an indication of proof of archival of an encryption key for the user in a database ~~under the control of an entity separate from the certificate authority~~;

verifying, by a registration manager, the digitally signed indication of proof;

sending, by the registration manager to the certificate authority, a request for a digital certificate based on the verifying; and

receiving, from the certificate authority, a digital certificate in response to the request.

11. (Canceled).

12. (Currently Amended) A method in a data processing system for archiving an encryption key ~~by a first entity other than a certificate authority~~, comprising:

receiving, from a registration manager, an encryption key for archiving;

archiving the received encryption key;

creating an indication of proof of archival of the received encryption key; and

providing the indication of proof of archival to the registration manager ~~a second entity~~ that verifies the indication of proof and provides a request for a digital certificate ~~from~~ to a ~~the~~ certificate authority based on a verified indication of proof.

13. (Original) The method of claim 12, further comprising the step of digitally signing the indication proof of archival.

14. (Currently Amended) The method of claim 13, wherein the archiving step further comprises ~~step~~ archiving the received encryption under control of a user.

15. (Currently Amended) A data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

a memory having program instructions; and

a processor configured to execute the program instructions to receive a request from a user for a digital certificate, receive, from an entity other than the certificate authority, an indication of proof of archival of the user's encryption key associated with the request, verify the indication of proof, wherein the user's encryption key is archived under control of ~~an~~ the entity ~~other than the certificate~~

~~authority~~, and ~~provide the~~ request ~~to~~ the digital certificate from the certificate authority based on the verification of the indication of proof.

16. (Currently Amended) A data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

a memory having program instructions; and

a processor configured to execute the program instructions to verify a received encrypted indication of proof that an encryption key for a user has been archived, send a request for a digital certificate to the certificate authority, the request ~~having~~ including the ~~a~~ verified indication of proof of archival of ~~an~~ the encryption key for the user ~~in an entity separate from the certificate authority~~, and receive, from the certificate authority, a digital certificate in response to the request.

17. (Currently Amended) A data processing system for archiving an encryption key by an entity other than a certificate authority, comprising:

a memory having program instructions; and

a processor configured to execute the program instructions to receive from a registration manager an encryption key for archiving, archive the received encryption key, create an indication of proof of archival of the received encryption key, encrypt the indication of proof, and send the encrypted indication of proof of archival to ~~an entity~~ the registration manager that verifies the indication of proof and

provides a request for a digital certificate to the certificate authority based on ~~a~~ the verification of the indication of proof ~~of archival~~.

18. (Original) A data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key under control of an entity other than the certificate authority, comprising:

a registration manager configured to receive a digital certificate request including a user's encryption key, send the user's encryption key, and in response receive an indication of proof of archival of the user's encryption key;

a data recovery manager configured to receive the user's encryption key, send the user's encryption key to a database controlled by an entity other than the certificate authority for archiving, create ~~an~~ the indication of proof of archival, and send the indication of proof of archival to the registration manager; and

a certificate authority configured to receive, from the registration manager, a request for a digital certificate for the user, the request including the indication of proof of archival, and issue a digital certificate when it is determined that ~~an~~ the indication proof of archival was received.~~; and~~

~~a database, under control of an entity other than the certificate authority, configured to receive and archive the user's encryption key.~~

19. (Currently Amended) A computer-readable medium containing instructions for controlling a data processing system to perform a method for

requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, the method comprising the steps of:

receiving, at a registration manager, a request including a user's encryption key from a user for a digital certificate;

receiving, by the registration manager, an indication of proof of archival of the user's encryption key associated with the request, wherein the user's encryption key is archived under control of an entity other than the certificate authority;

verifying, by the registration manager, the indication of proof; and

providing by the registration manager a second request including the verified indication of proof to the certificate authority;

receiving, by the registration manager, a digital certificate from the certificate authority based on the verified indication of proof; and

providing the received digital certificate to the user.

~~wherein the data processing system comprises a data recovery manager separate from the certificate authority that receives and manages archiving of the encryption key, and wherein the user's encryption key is encrypted during transmission from the user using the data recovery manager's public transport key~~.

20. (Canceled)

21. (Currently Amended) The computer-readable medium of claim 19, wherein the ~~data processing system includes a registration manager separate~~

~~from the certificate authority that sends the encrypted user's encryption key to the~~ entity is a data recovery manager.

22. (Canceled)

23. (Canceled)

24. (Canceled)

25. (Original) The computer-readable medium of claim 19, wherein the indication of proof of archival is digitally signed, and wherein the method further comprises the step of verifying a digital signature on the indication of proof of archival.

26. (Currently Amended) The computer-readable medium of claim 25, wherein the ~~data recovery manager~~ entity digitally signs the proof of archival.

27. (Original) The computer-readable medium of claim 19, wherein the user's encryption key is archived under control of the user.

28. (Currently Amended) A computer-readable medium containing instructions for controlling a data processing system to perform a method for

requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, the method comprising the steps of:

receiving a user encryption key from a registration manager that manages certificates for the user;

digitally signing an indication of proof of archival of ~~an~~ the user's encryption key ~~for the user~~ in a database under the control of an entity separate from the certificate authority;

providing the signed indication of proof to the registration manager;

verifying, by the registration manager, the digitally signed indication of proof;

sending, by the registration manager, a request for a digital certificate based on the verified digitally signed indication of proof; and

receiving, by the registration manager, a digital certificate in response to the request.

29. (Canceled)

30. (Previously Presented) A computer-readable medium containing instructions for controlling a data processing system to perform a method for archiving an encryption key by first entity other than a certificate authority, the method comprising the steps of:

receiving an encryption key for archiving;

archiving the received encryption key;

creating an indication of proof of archival of the received encryption key; and

providing the indication of proof of archival to a second entity that provides a request for a digital certificate from the certificate authority based on a verification of the indication of proof.

31. (Original) The computer-readable medium of claim 30, wherein the method further comprises the step of digitally signing the indication proof of archival.

32. (Original) The computer-readable medium of claim 31, wherein the archiving step further comprises the step of archiving the received encryption key under control of a user.

33. (Currently Amended) A data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

a registration manager including:

means for receiving a request from a user for a digital certificate, the request including an encryption key associated with the user that is encrypted using a first archival key;

~~means for encrypting the user's encryption key with a first archival key;~~

a recovery manager including:

means for storing the encrypted user's encryption key in a database ~~under the control of a first entity separate from the certificate authority~~;

means for providing an indication of proof of storing the encrypted user's encryption key, wherein the indication of proof is signed with a second archival key;

wherein the registration manager further includes means for verifying the signed indication of proof based on the first archival key**[[;]]** and means for providing the request to the certificate authority based on the verification of the signed indication of proof.